REMARKS/ARGUMENTS

This Amendment is in response to the Office Action dated September 9, 2004. Claims 1-32 are pending. Claims 1, 16, 31, and 32 have been amended. Accordingly, claims 1-32 remain pending in the present application.

The specification has been amended to insert missing serial numbers of related applications. Claims 1, 16, 31, and 32 have been amended to correct a typographical error by inserting the term "node" after the "second client." Claims 1 and 31 have further been amended to cancel the phrase "the steps of." Accordingly, it is respectfully submitted that no new matter has been entered. This amendment is seen by Applicant as broadening or cosmetic, and as such, is not subject to the prosecution history estoppel imposed by Festo. For the record, Applicant points out that the Supreme Court in Festo noted that a cosmetic amendment would not narrow the patent's scope and thus would not raise the estoppel bar.

The Examiner rejected claims 1-32 under 35 USC §103(a) as being unpatentable over Scott et al. (US publication number 2002/0049760) in view of Farber et al. (US patent number 5,978,791). Applicant respectfully disagrees.

The present invention provides a method and system for electronically delivering files in a peer-to-peer network comprising a server node and a plurality of client nodes. In a first aspect of the present invention, the method and system enable secure and reliable peer-to-peer file sharing between two client nodes. First, a digital fingerprint is generated and associated with a file in response to the file being selected for publication on a first client node. An entry for the file is then added to a searchable index of shared files on the server node, and the fingerprint for the file is also stored on the server. In response to a second client selecting the file from the search list on the server node, the file is automatically transferred from the first client node directly to the second client node. The second client node then generates a new fingerprint for the file and compares the new fingerprint with the fingerprint from the server node, thereby verifying the authenticity of the file and publisher.

In a second aspect of the present invention, the method and system enables subscription-based decentralized file downloads to the client nodes. First, the client nodes are allowed to subscribe with the server node to periodically receive copies of one of the files. To provide a current subscribing client node with the file, the geographically closest client node containing the file is located, and the file is transferred from the closest node directly to the current subscribing node, thereby efficiently utilizing bandwidth.

The Examiner cited Scott for teaching generating and associating a digital fingerprint with a file, storing the fingerprint of the file in a server, and for transferring the file from one client node to another. Applicant agrees with the Examiner that Scott fails to teach or suggest "generating a new fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity of the file and publisher," as recited in the independent claims. The Examiner cited Farber for teaching this step.

Scott teaches a data processing system, including a peer-to-peer network, in which a unique identifier called a "True Name") is generated for a data item using only the data in the data item. Farber, however, also fails to teach or suggest “generating a new fingerprint for a file” after the file is transferred to a client node “and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity of the file and publisher," as recited in the claimed invention. The Examiner cites Farber column 12, lines 54-67 through column 13, lines 1-18 for teaching these features. However, this passage of Farber only states:

> 1. Calculate True Name
>
> A True Name is computed using a function, MD, which reduces a data block B of arbitrary length to a relatively small, fixed size identifier, the True Name of the data block, such that the True Name of the data block is virtually guaranteed to represent the data block B and only data block B.
>
> The function MD must have the following properties:
>
> 1. The domain of the function MD is the set of all data items. The range of the function MD is the set of True Names.
>
> 2. The function MD must take a data item of arbitrary length and reduce it to an integer value in the range 0 to N-1, where N is the cardinality of the set of True Names. That is, for an arbitrary length data block B, 0.ltoreq.MD(B).ltoreq.N.
>
> 3. The results of MD(B) must be evenly and randomly distributed over the range of N, in such a way that simple or regular changes to B are virtually guaranteed to produce a different value of MD(B).
>
> 4. It must be computationally difficult to find a different value B' such that MD(B)=MD(B').
>
> 5. The function MD(B) must be efficiently computed.
>
> A family of functions with the above properties are the so-called message digest functions, which are used in digital security systems as techniques for authentification of data. These functions (or algorithms) include MD4, MD5, and SHA.
>
> In the presently preferred embodiments, either MD5 or SHA is employed as the basis for the computation of True Names. Whichever of these two message digest functions is employed, that same function must be employed on a system-wide basis.
>
> It is impossible to define a function having a unique output for each possible input when the number of elements in the range of the function is smaller than the number of elements in its domain. However, a crucial observation is that the actual data items that will be encountered in the operation of any system embodying this invention form a very sparse subset of all the possible inputs.

As can be seen, the cited passage of a Farber only describes the mechanism by which a True Name is calculated for a data item or file using algorithms such as MD or SHA. Calculation of the True Name is but one of several primitive mechanisms that

Farber provides for use in a file system of a data processing system (col. 6, lines 11-19). Farber describes the following primitive mechanisms: 1. Calculate True Name; 2. Assimilate Data Item; 3. New True File; 4. Get True Name from Path; 5. Link Path to True Name; 6. Realize True File from Location; 7. Locate Remote File; 8. Make True File Local; 9. Create Scratch File; 10. Freeze Directory; 11. Expand Frozen Directory; 12. Delete True File; 13. Process Audit File Entry; 14. Begin Grooming; 15. Select For Removal; and 16. End Grooming (col. 6, lines 28-46).

Nothing in the description for the True Name primitive, or any other of the other primitive mechanisms, teaches or suggests that once a file is transferred from one client node to another in a peer-to-peer network, that the client node to which the file is transferred generates a *new* fingerprint/True Name for the file and then *compares* it with the fingerprint/True Name stored on a server, as recited in claims 1, 16, 31, and 32.

Farber describes that the assimilation mechanism is for adding a given data item to the file registry. This is done by determining the True Name of the data item corresponding to a scratch file and then looking for an entry for the True Name in a True File registry and determining whether a True Name record exists. If a record exists, the scratch file is deleted. Otherwise the True File ID for the scratch file is stored in the entry record (col. 7, lines 41-50).

Although in the instance where a True Name is generated for a file that already has an existing record the True Name is generated twice, the time when the True Name is generated and the reason for generating the True Name in Farber is different than the time when the new fingerprint is generated and the reason for generating the new fingerprint in the present invention.

The time at which the True Name is generated in Farber is when a file is being added to the system and the reason for generating the True Name is to check for a duplicate entry. In contrast, in the present invention, the time at which a new fingerprint is generated is after one client node selects a file to download from a search list and then receives the file from another client node, and the reason for generating the new fingerprint is to "determine the authenticity of the file and the publisher," which includes ensuring that the contents of the file have not been tapered with since publication.

Although both Scott and Farber may teach the generation of a fingerprint for a file, neither Scott or Farber, singularly or in combination, teach or suggest generating a new fingerprint for a previously existing file in the system; generating the new fingerprint in response to the file being transferred from one client node to the other in a peer-to-peer network, or the purpose for the new fingerprint, as recited in claims 1, 16, 31, and 32.

Further with respect the purpose of the new fingerprint, the combination of Scott and Farber also fails to teach or suggest using the new fingerprint to "determine the authenticity of... *the publisher*," as recited. Scott's stated purpose for generating the fingerprint ID is "to identify identical files stored in a peer-to-peer network which have different filenames and/or other metadata descriptors, and to use the fingerprint ID to retrieve the desired content from one or more of the identified files [0008]. Farber's stated purpose for generating the True Name is to identify "a data item in the system, where the identity of the data item depends on all the data in the data item and only on the data in the data item" (col. 1, lines 28-34). The combination of Scott and Farber fails to teach or suggest using the fingerprint or True Name to determine the authenticity of the "publisher" of the file, as recited in claims 1, 16, 31, and 32.

The authenticity of the publisher in the present invention is established by incorporating publisher information in the fingerprint. As described in the specification, each user of the P2P network is required to register with the network and account information is generated for the user including a digital certificate that includes a public key and a private key. When the user publishes a file, a bitstream ID is generated for the file, and the user's private key is used to generate a digital signature for the file. In one embodiment, the bitstream ID 34, the file information, and the digital signature 40 form the fingerprint for the file. The fingerprint ensures that the file is transmitted in its original state (data integrity) by the identified user/publisher (page 10, line 20 through page 11, line 8).

The above described steps are recited in claims 3-6 and 18-21. Neither Scott or Farber disclose using public/private key encryption and assigning a private key to each user of a peer-to-peer network, using the private key to create a digital certificate, using the digital certificate to generate a fingerprint for each file when the file is published, and then generating a new fingerprint by the client nodes upon receipt of the file "to determine the authenticity of the file and publisher.

More specifically, the combination of Scott and Farber fails to teach or suggest "generating account information for a user, including a digital certificate, in response to a registration process, wherein the digital certificate includes a private key and a public key," as recited in claims 3 and 18; "generating a bitstream ID for the file and including the bitstream ID in the fingerprint," as recited in claims 4 and 19; "using the private key to generate a digital signature from the file and including the digital signature in the fingerprint," as recited in claims 5 and 20; and "authenticating the file by generating a new bitstream ID and comparing the new bitstream ID to the bitstream ID in the fingerprint stored on the server, and using the user's public key to decrypt the digital signature," as recited in claims 6 and 21.

In the rejection of claims in 3 and 18, the Examiner took Official notice that it is well-known in the art to generate a digital certificate that includes a private key and a public key. Although this may be, digital certificates are typically used for encrypting data for security reasons. The Examiner has failed to cite any art that teaches or suggests the incorporation of a digital certificate of a publisher into a fingerprint for a file so that client nodes in a peer-to-peer network can determine the authenticity of the publisher when the file is transferred from node to another node. Absent any teaching or suggestion to the contrary, it is believed claims 1, 3-6, 16, 18-21, 31, and 32 are allowable over the cited references.

Referring now to claims 2, 17, 31, and 32, it is respectfully submitted that a combination of Scott and Farber also fails to teach or suggest "enabling subscription-based decentralized file downloads," as claimed. The Examiner cited Scott, page 4, paragraphs [0046]-[0049] and page 3, paragraph [0034] for teaching subscription-based decentralized file downloads. As described below, however, the cited paragraphs fail to disclose such.

Paragraph [0046] describes the process of a requesting peer choosing a file to download from a list of locations; paragraph [0047] describes that once the requesting peer has chosen a first location to start retrieving the file from (e.g., peer2) the requesting peer makes a request operation to the second peer for file that has a desired hash ID, and the requesting peer transmits the contents of the requested file; paragraph [0048] describes that the name and metadata of the file selected in the search results may not necessarily be the same as the name and metadata attached to the file by the second peer, and that the requesting peer notifies the server that it has a copy of the file to become a for filling peer for a subsequent request for the same file; and paragraph [0049] describes that when the fulfilling peer is no longer online, the requesting peer will select the next location peer (peer3) from the list of available locations. And Paragraph [0034] describes that the central directory data, which includes a file directory table, may be stored in a relational database, and further describes the contents of the tables.

Nothing in the paragraphs cited by the Examiner teaches or suggests "allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files... and transferring files from the closest node directly to the current subscribing node" as recited in claims 2, 17, 31, and 32. In fact, Applicant has performed a keyword search on Scott and the terms “subscription” and “subscribe” were not found. Appendix C of Scott on page 8 of 53 includes the term “Auto-Update” and page 49 of 53 includes the terms “Fileclubs”, but no descriptions or definitions of the terms are provided. Therefore, it is difficult for the Applicant to ascertain whether or not the terms “Auto-Update” and “Fileclubs” are analogous to the claimed “subscription-based decentralized file downloads.” In any event, even if the terms “Auto-Update” and “Fileclubs” were considered analogous to subscriptions, it is respectfully submitted that Scott's “Auto-Update” and “Fileclubs” feature are not taught in combination with a client node “generating a new fingerprint” in response to receiving a file from another client node in order to “determine the authenticity of the file and publisher,” as recited in claims 2, 17, 31, and 32. Absent any teaching or suggestion to the contrary, it is respectfully submitted that claims 2, 17, 31 and 32 are allowable over Scott and Farber.

The arguments above apply with full force and effect to the remaining dependent claims because they are based on allowable independent claims. Therefore, the dependent claims are allowable for at least the same reasons as the independent claims.

In view of the foregoing, it is submitted that claims 1-32 are allowable over the cited references. Because the secondary references stand or fall with the primary references, claims are allowable because they are dependent upon the allowable independent claims. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 1-32 as now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

March 7, 2005

Stephen G. Sullivan
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540